

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-161354

(43)公開日 平成6年(1994)6月7日

(51)Int.Cl.⁵

G 0 9 C 1/00

G 0 6 K 17/00

識別記号

庁内整理番号

8837-5L

S 7459-5L

F I

技術表示箇所

審査請求 未請求 請求項の数2(全11頁)

(21)出願番号 特願平4-317255

(22)出願日 平成4年(1992)11月26日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72)発明者 石黒 銀矢

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72)発明者 牟田 敏保

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72)発明者 崎田 一貴

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74)代理人 弁理士 草野 卓

最終頁に続く

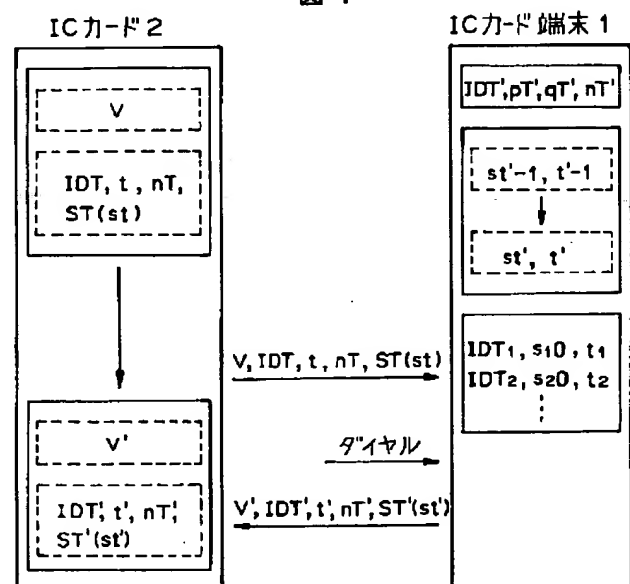
(54)【発明の名称】 ICカード端末及びそれを用いたシステム

(57)【要約】 (修正有)

【目的】 ICカード端末を用いた不正使用を防止する。

【構成】 ICカード2をICカード端末1に挿入すると、ICカードから残金額Vと前回使用した端末の番号IDT、タイムスタンプ情報stの更新回数を示す回数t、公開鍵nT、タイムスタンプの署名ST(st)とが端末へ送信される。盗難端末の番号と一致するものがない場合はVが利用者により指定されたサービス料金より高ければサービスを提供。サービス終了後Vから使用料金を引いた残りV'と、その端末のIDT'、更新情報t'、端末鍵pT'、qT'によるタイムスタンプ情報st'に対するデジタル署名ST'(st')、公開鍵nT'とをICカードへ送る。端末リストのIDT初期値を、受信したtだけ繰り返し演算してタイムスタンプ情報を更新これと鍵nTとにより署名STの正当性を検証、正当でなければ異常カードとし、正当であれば、ICカードが端末で使用された時期を判定する。

図4



【特許請求の範囲】

【請求項1】 適当な間隔で所定のアルゴリズムによりタイムスタンプ情報を更新する手段と、
上記タイムスタンプ情報の更新ごとにその更新回数を表す更新情報を管理センタへ送信する手段と、
端末を特定するための端末番号、上記タイムスタンプ情報、上記更新情報、デジタル署名を作成するための端末鍵、上記デジタル署名を検証するための公開鍵とを記録したメモリと、
上記管理センタから受信した端末番号、タイムスタンプ情報の初期値、更新情報が端末リストとして記録されるメモリと、
ＩＣカードから受信した端末番号と上記端末リストの端末番号との比較を行い、一致しているとその端末リストのタイムスタンプ情報の初期値を、上記ＩＣカードから受信した更新情報に応じて上記所定のアルゴリズムにより更新し、その更新したタイムスタンプ情報と、受信した公開鍵とにより上記ＩＣカードから受信したデジタル署名の検証を行い、正当と判断したとき、上記受信した更新情報と上記一致した端末番号の端末リストの更新情報との比較を行い、上記ＩＣカードが上記受信した端末番号のＩＣカード端末で使用された時期を判断する手段と、
上記更新されたタイムスタンプ情報を上記端末鍵を用いてデジタル署名する手段と、
上記端末を特定するための端末番号、上記更新情報、上記公開鍵、上記デジタル署名を上記ＩＣカードへ送信する手段と、
を具備するＩＣカード端末。

【請求項2】 上記請求項1記載のＩＣカード端末と、
ＩＣカード端末から受信されたその端末番号、更新情報、公開鍵、タイムスタンプ情報に対するデジタル署名を記録するメモリと、
ＩＣカード端末へ挿入すると上記メモリ中の端末番号、更新情報、公開鍵、タイムスタンプ情報に対するデジタル署名をそのＩＣカード端末へ送信する手段とを具備するＩＣカードと、
各ＩＣカード端末の端末番号、タイムスタンプ情報の初期値及び更新情報を管理するデータベースと、
上記ＩＣカード端末より受信された更新情報に、上記データベース中の対応端末番号の更新情報を置き換える手段と、
上記データベース中の端末番号、タイムスタンプ情報の初期値及び更新情報の1組を選択してすべてのＩＣカード端末へ送信する手段と、を具備する管理センタと、
よりなるＩＣカードシステム。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 この発明はＩＣカードをプリペイドカード、クレジットカード、スタンプカードなどとし

て使用するシステム、及びそのＩＣカード端末に関する。

【0002】

【従来の技術】 従来この種のシステムは、ＩＣカードとＩＣカード端末とが同じ暗号方式で、同じ秘密鍵を持ち、金額情報をこの秘密鍵で暗号化して通信し、各々の秘密鍵はＩＣカードやＩＣカード端末の内部を開けても、秘密鍵を見たり、改ざんしたりできないようにしていた。したがって、秘密鍵が漏洩しない限りＩＣカードの内容を改ざんすることはほとんど不可能であった。

【0003】

【発明が解決しようとする課題】 しかしながら、盗んだＩＣカード端末を用いてＩＣカードの内容を不正に書き換えることは不可能とは言えず、一旦可能となった場合にはシステムダウンといった重大な影響を及ぼす危険性がある。

【0004】

【課題を解決するための手段】 請求項1の発明は端末を特定するための端末番号、適当な間隔で所定のアルゴリズムにより更新されるタイムスタンプ情報、そのタイムスタンプ情報の更新回数を表す更新情報、デジタル署名を作成するための端末鍵、そのデジタル署名を検証するための公開鍵を記録したメモリ、管理センタから受信した端末番号、タイムスタンプ情報の初期値、更新情報を端末リストとして記録するためのメモリ、ＩＣカードから受信した端末番号と前記端末リストに記録している端末番号との比較を行い、一致したとき端末リストに記録しているその端末番号に対応するタイムスタンプ情報の初期値をＩＣカードから受信した更新情報にしたがい前記所定のアルゴリズムにより更新し、その更新したタイムスタンプ情報とＩＣカードから受信した公開鍵とにより受信したデジタル署名の検証を行い、正当と判断したとき、受信した更新情報と端末リストに記録しているその端末番号に対応する更新情報との比較を行い、そのＩＣカードが受信した端末番号のＩＣカード端末で使用された時期を判断する手段を持つＩＣカード端末である。

【0005】 請求項2の発明によれば請求項1の発明のＩＣカード端末と、ＩＣカード端末での使用後に、そのＩＣカード端末の前記端末番号、前記更新情報、前記タイムスタンプ情報を含む情報に対するデジタル署名、前記公開鍵を受信してメモリに記録する手段、次の使用時に、前記メモリに記録している端末番号、更新情報、デジタル署名、公開鍵をＩＣカード端末へ送信する手段を持つＩＣカードと、各ＩＣカード端末の端末番号、タイムスタンプ情報の初期値および更新情報を管理するデータベース、ＩＣカード端末がそのタイムスタンプ情報を更新するごとにそのＩＣカード端末から更新情報を受信し、その端末番号に対応して記録している更新情報を受信した更新情報に置き換える手段を持つ管理センタとによりＩＣカードシステムが構成されている。

【0006】

【作用】このように構成しているから、ICカードを使用したとき、ICカード内の所定のメモリエリアに、使用したICカード端末の端末番号、そのICカード端末が作成したデジタル署名を検証するための公開鍵、使用時点のタイムスタンプ情報に対してそのICカード端末が作成したデジタル署名、そのタイムスタンプ情報の更新情報とを記録する。次に別のICカード端末で使ったとき、ICカードは前記メモリに記録した情報をICカード端末へ送信し、ICカード端末は受信した端末番号から前回使用したICカード端末を特定する。その端末番号とICカード端末内の端末リストに登録されている端末番号との比較を行い、一致するものがあるとき、その端末リストに登録されているその端末番号に対応したタイムスタンプ情報の初期値と更新情報を読み出し、そのタイムスタンプ情報の初期値をICカードから受信した更新情報にしたがって所定のアルゴリズムにより更新して前回使用した時点でのICカード端末のタイムスタンプ情報を求める。その求めたタイムスタンプ情報とICカードから受信した公開鍵とによりタイムスタンプ情報に対するデジタル署名の正当性を検証し、ICカードから受信した更新情報が正しい値であることをチェックする。その更新情報が正当であるとき、その更新情報と前記端末リストに登録されている更新情報を比較し、ICカードの前記端末リストに登録されているICカード端末での使用時期が、前記端末リストに端末番号を登録した時点よりも以前か、以後かを判断する。デジタル署名の検証において正当性を検証できなかったときには、ICカードから受信した更新情報あるいはデジタル署名が正規の情報ではないと判断し、異常カードとして処理する。さらに、管理センタでICカード端末の端末番号を指定すれば、その端末番号のICカード端末のタイムスタンプ情報の初期値、その時点での更新情報を知ることができ、それらの情報をICカード端末の端末リストに登録することができる。

【0007】

【実施例】次に図を参照してこの発明の一実施例をブレイドカードシステムに適用した場合につき説明する。図1は請求項2の発明の一実施例のシステム構成の説明図であって、ICカード端末1はICカード2により料金処理を実施し、通話など各種サービスを提供する。管理センタ3はICカード端末1の端末番号などを管理し、ICカード端末1の電話番号へ発呼することによりICカード端末1と管理センタ3とは通信網4を介して接続され、情報を送信することができる。

【0008】図2は請求項1の発明のICカード端末1の内部構成を示す図であり、制御部11はCPUからなり、処理手順、タイムスタンプ情報を更新するためのアルゴリズム、デジタル署名を作成するためのアルゴリズムなどのプログラムを内部のROMに記録していると

もに、端末番号、タイムスタンプ情報、タイムスタンプ情報の更新情報、デジタル署名を作成するための端末鍵、デジタル署名を検証するための公開鍵などを内部RAMに記録している。タイムスタンプ情報を更新するアルゴリズムとしては、例えば「電子情報通信学会論文誌D分冊, J70-D, No. 7, p. 1413~1423 (1987)」に記載のFEALを用いてもよく、デジタル署名のアルゴリズムとしては、例えば「NTT R&D Vol. 40, No. 5, p. 687~696 (1991)」に記載のESIGNを用いることができる。端末番号、タイムスタンプ情報の初期値、端末鍵、公開鍵は、ICカード端末設置時に、通信網を介して管理センタ3(図示せず)と接続し、管理センタ3から受信してメモリに記録してもよく、ICカード端末製造時に予め設定してもよい。更新情報は例えば初期値として0を設定し、タイムスタンプ情報を更新するごとに1, 2, ...と増加していく。また、内部RAMには特定のICカード端末の端末番号、タイムスタンプ情報の初期値、更新情報を登録するための端末リストエリアが設けられている。ICカード2とデータのやりとりを行うICカードリーダライタ部12、操作ボタン、ダイヤルボタンなどからなる操作入力部13、液晶ディスプレイからなる表示部14、通話回路15は制御部11に接続され、通話回路15に送受器16が接続され、通信網との処理を行う通信処理部17が制御部11に接続されている。

【0009】図3はICカード2の内部構成を示す図であり、ICカードの処理手順、デジタル署名の検証のためのアルゴリズム等のプログラムはROM61に記録され、CPU63はワークエリアとしてRAM62を利用してすべての制御を行い、図2に示したICカード端末1のICカードリーダライタ部12との通信は通信部65により接点66を介して行われる。金額情報はICカード2の発行時にICカード発行機(図示せず)によって書き込まれ、EEPROM64に記録されている。

【0010】図1から図3の構成において、ICカード端末1に設定した端末番号、タイムスタンプ情報の初期値、更新情報は管理センタ3に登録される。ICカード端末1に設定したタイムスタンプ情報(初期値)は内部の時計機能により、例えば1日ごとに所定のアルゴリズムにより更新され、 $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots \rightarrow s_t$ のごとく新しいタイムスタンプ情報に置き換えられ、前のタイムスタンプ情報は消滅する。このタイムスタンプ情報の更新は1定周期ごとでなくてもよく、つまり非周期的でもよい。タイムスタンプ情報を更新するごとに、更新した回数を更新情報として置き換える各タイムスタンプ情報と更新情報とが対応していればよく、つまりタイムスタンプ情報は単なる記号で、数量でなくても各更新回数とタイムスタンプ情報とが1対1で対応していればよい。更新情報を更新したとき、ICカード端末1から管

理センタ 3 に自動発信し、端末番号と更新した更新情報を送信する。管理センタ 3 は登録されている対応端末番号の更新情報を、受信した更新情報に置き換える。なお、タイムスタンプ情報を更新する所定のアルゴリズムとしては、現在のタイムスタンプ情報から、前のタイムスタンプ情報を求めることができないようなアルゴリズムとすることが必要である。また、管理センタ 3 に登録されたタイムスタンプ情報の初期値は更新されない。このような状態において、ICカード端末の盗難が発生した時、管理センタ 3 は盗まれた IC カード端末の端末番号から、その IC カード端末のタイムスタンプ情報の初期値、盗まれた時点のタイムスタンプ情報の更新情報を知ることができ、それらの情報は管理センタ 3 からダウンロードにより全 IC カード端末 1 の端末リストに登録される。

【0011】図 4 は利用者が IC カード 2 を使って IC カード端末 1 からサービスを受けるときの処理を説明する図である。IC カード 2 の EEPROM 64 の所定のエリアに金額情報 V が記録され、他の所定のエリアには前回使用した IC カード端末の端末番号 IDT 、公開鍵 nT 、更新情報 t 、タイムスタンプ情報に対するデジタル署名 $ST(st)$ が記録されている。また、IC カード端末 1 の制御部 11 内の RAM の所定のエリアに端末番号 IDT' 、デジタル署名用の端末鍵 pT' 、 qT' 、公開鍵 nT' が記録され、他の所定のエリアにはタイムスタンプ情報 sT' 、更新情報 t' が記録されている。更に、IC カード端末 1 の端末リストには、特定の端末の端末番号 IDT_i ($i=1, 2, \dots$)、タイムスタンプ情報の初期値 $s_i 0$ 、更新情報 t_i が記録されている。

【0012】利用者が IC カード 2 を IC カード端末 1 の IC カードリーダライタ部 12 に挿入すると IC カード 2 から IC カード端末 1 に V 、 IDT 、 t 、 nT 、 $ST(st)$ が送信される。IC カード端末 1 は受信した IDT と端末リスト内のデータ IDT_i との比較を行い、一致するものがない場合には V 及びガイダンスを表示部に表示する。利用者は表示部 14 に表示されたガイダンスを参照して、操作入力部 13 からダイヤルなどによりサービスを指定すると、IC カード端末 1 は指定されたサービスの料金を制御部 11 内のメモリに記憶されているリストの中から読み取るか、あるいは、通信網 4 を介して図示していないサービスセンタから受信し、この必要なサービス料金と残金額 V を比較して、 V が大きければサービスの提供を開始する。たとえば、電話サービスであれば残金額が 10 円以上であればダイヤル指示を表示部 14 に表示し、利用者のダイヤルに従って相手に発信する。利用者がサービスの提供を受け、例えば相手との通話が終了したサービス終了後は、IC カード端末 1 は制御部 11 内のメモリにあるサービス料金結果あるいはサービスセンタから送信されるサービス料金結果を

前記残金額 V から減算して新しい残金額 V' を求め、タイムスタンプ情報 sT' に対してデジタル署名 $ST'(st')$ を端末鍵 pT' 、 qT' で作成し、 IDT' 、 V' 、 t' 、 nT' 、 $ST'(st')$ を IC カード 2 へ送信する。IC カード 2 は残金額 V' とともに IC カード端末 1 から受信した情報を EEPROM 64 に記録する。

【0013】上記の処理において、IC カード端末 1 が受信した IDT と一致するデータが端末リスト内のデータ IDT_i にあった場合には、次の処理を行う。

① IDT_1 が一致した端末番号とすると、端末リスト内の一致した端末番号に対応するタイムスタンプ情報の初期値 $s_1 0$ を、IC カード端末 1 のプログラムとして記録されている所定のアルゴリズムにより、IC カード 2 から受信した更新情報 t に従い、その更新回数だけ繰り返し演算を行い、この t と対応したタイムスタンプ情報 s 、 t を求める。

【0014】

$s_1 0 \rightarrow s_1 1 \rightarrow s_1 2 \dots \dots \dots \rightarrow s_1 t$

② この演算により求めたタイムスタンプ情報 s_{t1} と、IC カード 2 から受信した公開鍵 nT とによりデジタル署名 $ST(st)$ の正当性の検証を行う。

③ 正当性が検証できなかった場合には、異常カードとして処理を中止し、IC カード 2 を返却する。

④ 正当性が検証できた場合には、端末リスト内の一致した端末番号 IDT_1 に対応する更新情報 t_1 と、IC カード 2 から受信した更新情報 t との比較を行う。

⑤ $t \leq t_1$ の場合には、その t は IDT_1 、 $s_1 0$ 、 t_1 が端末リストに登録される前の更新情報であると、すなわちその IC カードは、その IDT_1 の IC カード端末が盗難される前にその IC カード端末でデータ（端末番号、更新情報、公開鍵、デジタル署名されたタイムスタンプ情報）が更新された IC カードであると判断され、正当なものとして以降の処理を行う。

⑥ $t > t_1$ の場合には、その t_1 は、 IDT_1 、 $s_1 0$ 、 t_1 が端末リストに登録された後の更新情報であると、すなわちその IC カードは、その IDT_1 の IC カード端末が盗難された後にその IC カード端末でデータが更新された IC カードであると判断され、不正カードとして処理を中止し、返却あるいは IC カード端末内への留置処理を行う。

【0015】図 5 はこの発明の他の実施例を説明する図であって、IC カード 2 の ROM 61 にはデジタル署名を作成するためのアルゴリズム、乱数を生成するためのアルゴリズムが記録されている。また、IC カード 2 の EEPROM 64 にはカード番号 IDU 、デジタル署名を作成するためのカード鍵 pU 、 qU 、デジタル署名を検証するための公開鍵 nU が記録されている。EEPROM 64 の所定のエリアには前回使用した IC カード端末の端末番号 IDT 、公開鍵 nT 、更新情報 t 、前回の

使用時に生成された乱数RおよびX、とともにこれら乱数R、X、金額情報V、カード番号IDUに対して前回使用したICカード端末が作成した第1のデジタル署名 $ST(R * X * V * IDU)$ 、そのデジタル署名およびタイムスタンプ情報stに対して前回使用したICカード端末が作成した第2のデジタル署名 $ST(st * ST(R * X * V * IDU))$ が記録されている。また、ICカード端末1の制御部11内のROMには乱数を生成するためのアルゴリズムが記録されている。

【0016】利用者がICカード2をICカード端末1のICカードリーダライタ部12に挿入すると、ICカード2からICカード端末1に前回使用情報であるR、X、V、IDU、第1のデジタル署名、IDT、t、nT、第2のデジタル署名が送信される。ICカード端末1は受信したnTにより第1のデジタル署名の正当性を検証する。正当であれば、受信した端末番号IDTと端末リスト内のデータとの比較を行い、一致するものがない場合には乱数R'を生成しICカードへ送信する。ICカードでは乱数X'を生成するとともにR'、X'、Vに対して鍵pU、qUによりデジタル署名SU($R' * X' * V$)を作成し、X'、SU($R' * X' * V$)、nUをICカード端末1へ送信する。ICカード端末1では受信した公開鍵nUによりデジタル署名SU($R' * X' * V$)の正当性を検証する。正当であればVを表示部に表示し所定のサービスを提供する。そのサービス終了後、新しい残金額V'を求め、R'、X'、V'、IDUに対して鍵pT'、qT'により第1のデジタル署名ST'($R' * X' * V' * IDU$)を作成するとともに、タイムスタンプ情報st'と第1のデジタル署名に対して第2のデジタル署名 $ST(st' * ST(R' * X' * V' * IDU))$ を作成し、V'、IDT'、nT、t'、第1のデジタル署名、第2のデジタル署名をICカード2へ送信する。ICカード2は受信したnT'により受信した第1のデジタル署名の検証を行い、正当であれば受信した情報を所定のエリアに記録する。以上の手順でデジタル署名の正当性が検証できなかった場合にはその時点で処理を中止し、ICカード2を返却する。

【0017】上記の処理において、ICカード端末1が受信したIDTと一致するデータが端末リスト内のデータIDTiにあった場合には、前述した処理と同様の処理を行う。この実施例では情報の送受に相互に生成した乱数を使用しているため信号の内容は同一となることはなく、傍受した信号を利用した不正を防止することができる。また、相互にデジタル署名を作成して相互認証を行っているためセキュリティをより高めることができ

る。なお情報の数が多い程、セキュリティが高くなるが、カード番号IDUを省略しても図4の場合より可成りよくなる。

【0018】以上の説明において、ICカード端末1およびICカード2はそれぞれ端末番号およびカード番号のみメモリに記録しているように説明してきたが、特定の鍵情報によって端末番号およびカード場合のデジタル署名を作成し、そのデジタル署名を検証鍵とともに各々のメモリに記録しておき、端末番号あるいはカード番号とともにそのデジタル署名、検証鍵も一緒に送信し、検証鍵によりデジタル署名を検証することにより端末番号あるいはカード番号の正当性を検証するように構成すればセキュリティをより高めることができる。

【0019】また、ICカード2およびICカード端末1に送信情報の暗号化・復号化のためのアルゴリズムと暗号化および復号化のための共通の鍵をメモリに記憶しておくことにより、相互の通信を暗号通信により行うことができ、よりセキュリティを高めることができる。

【0020】

【発明の効果】この発明によれば、ICカード端末が設置されてからの経過時間を表す更新情報と、更新情報の正当性を検証するためのタイムスタンプ情報をICカード端末に記録し、ICカードを使用すると、更新情報とともにタイムスタンプ情報の正当性を検証するためのそのICカード端末のデジタル署名をICカードに記録するため、ICカードの内容を解析して更新情報をもどすように改ざんしたとしても、その改ざんした更新情報と対応するタイムスタンプ情報に対するICカード端末のデジタル署名を作成することができないために不正はできない。また、ICカード端末の内容を解析して更新情報をもどすように改ざんしたとしても、もどした更新情報に対応するタイムスタンプ情報を得ることはできず、不正を行うことはできない。ICカード端末の解析によりできることは、その時点以降のタイムスタンプ情報、更新情報の付いた内容の改ざんとなり、他のICカード端末で使用した場合には、端末リストチェックにより不正を防ぐことができる。

【図面の簡単な説明】

【図1】請求項2の発明の一実施例のシステム構成を示すブロック図。

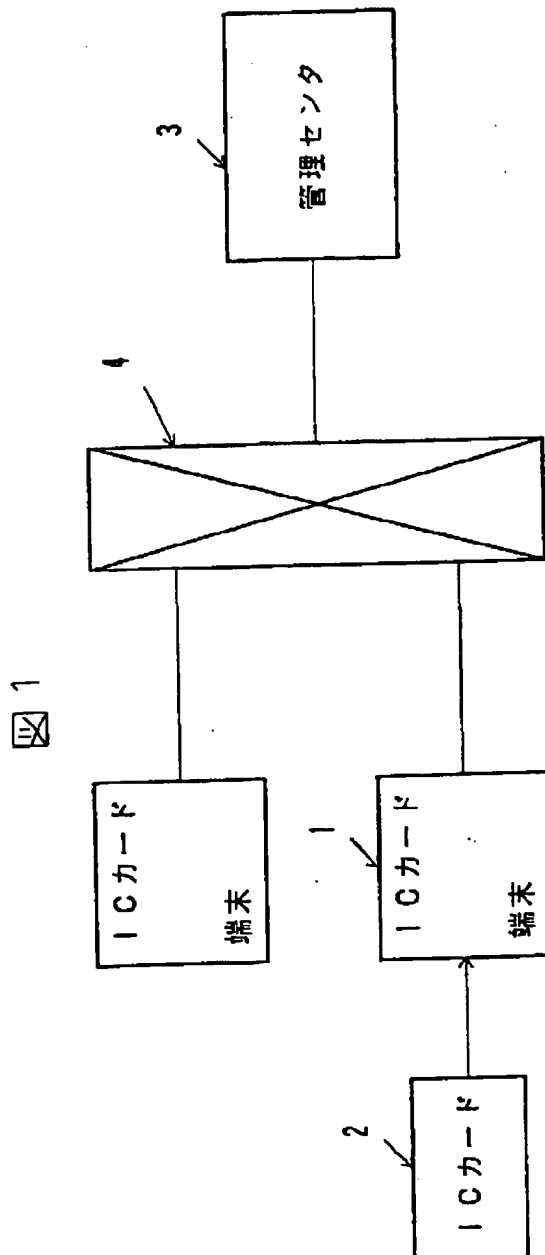
【図2】請求項1の発明のICカード端末の構成例を示すブロック図。

【図3】ICカードの構成例を示すブロック図。

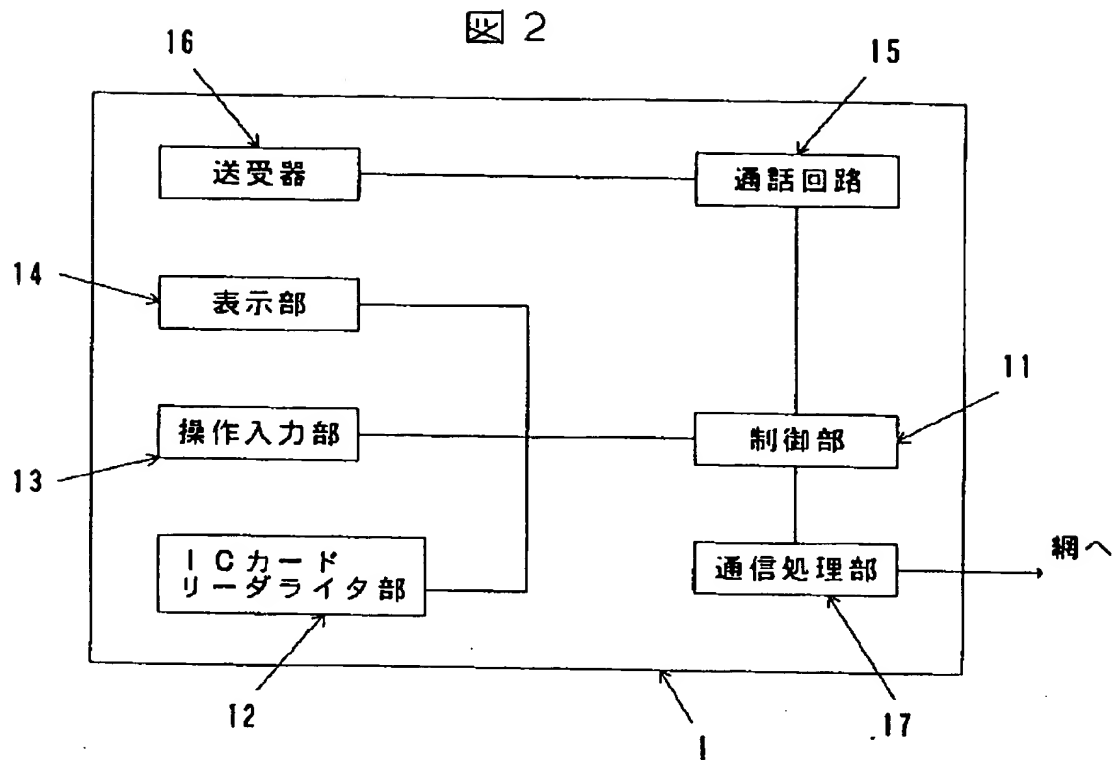
【図4】この発明の情報処理手順の例を示す図。

【図5】この発明の他の情報処理手順を示す図。

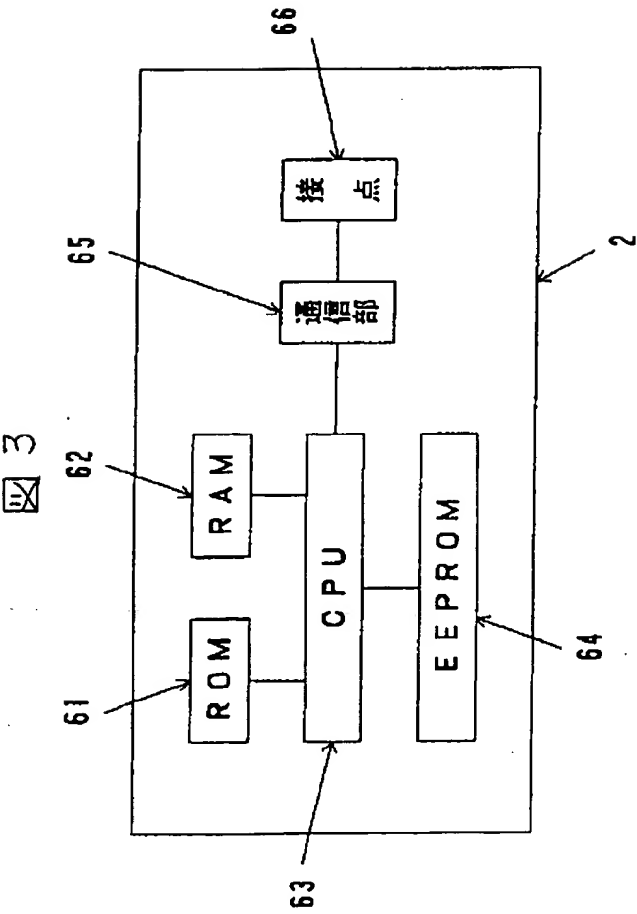
【図1】



【図2】

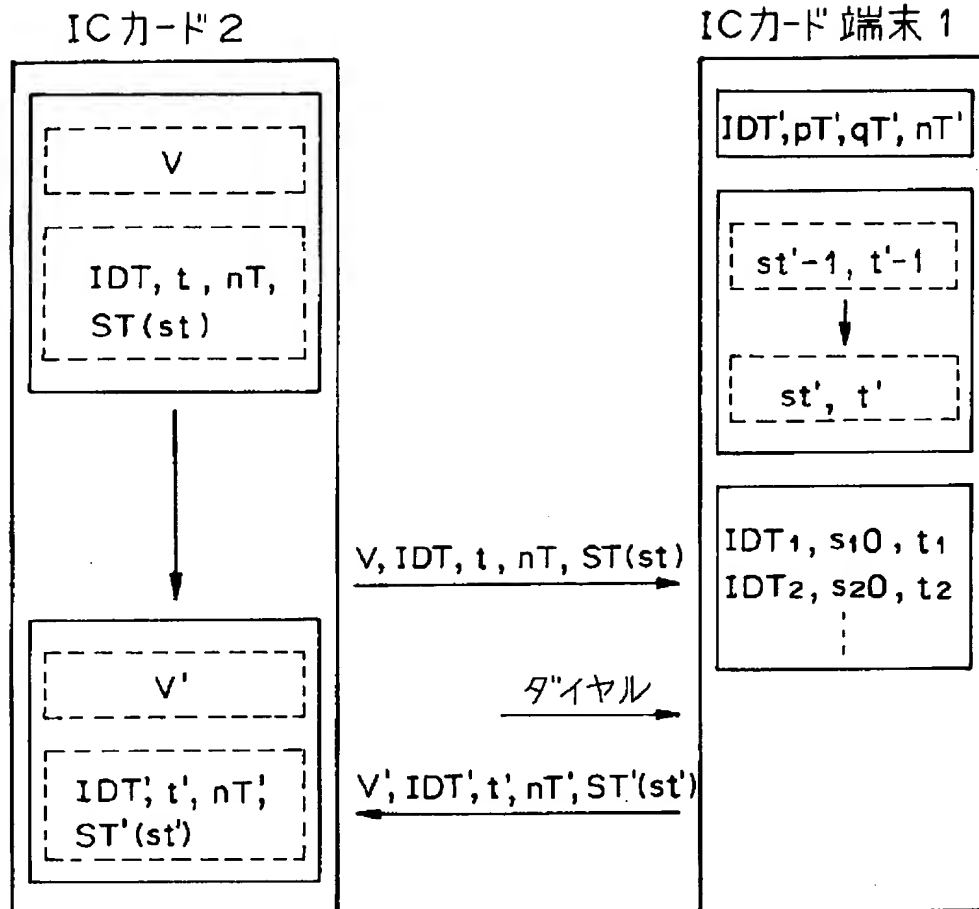


【図3】

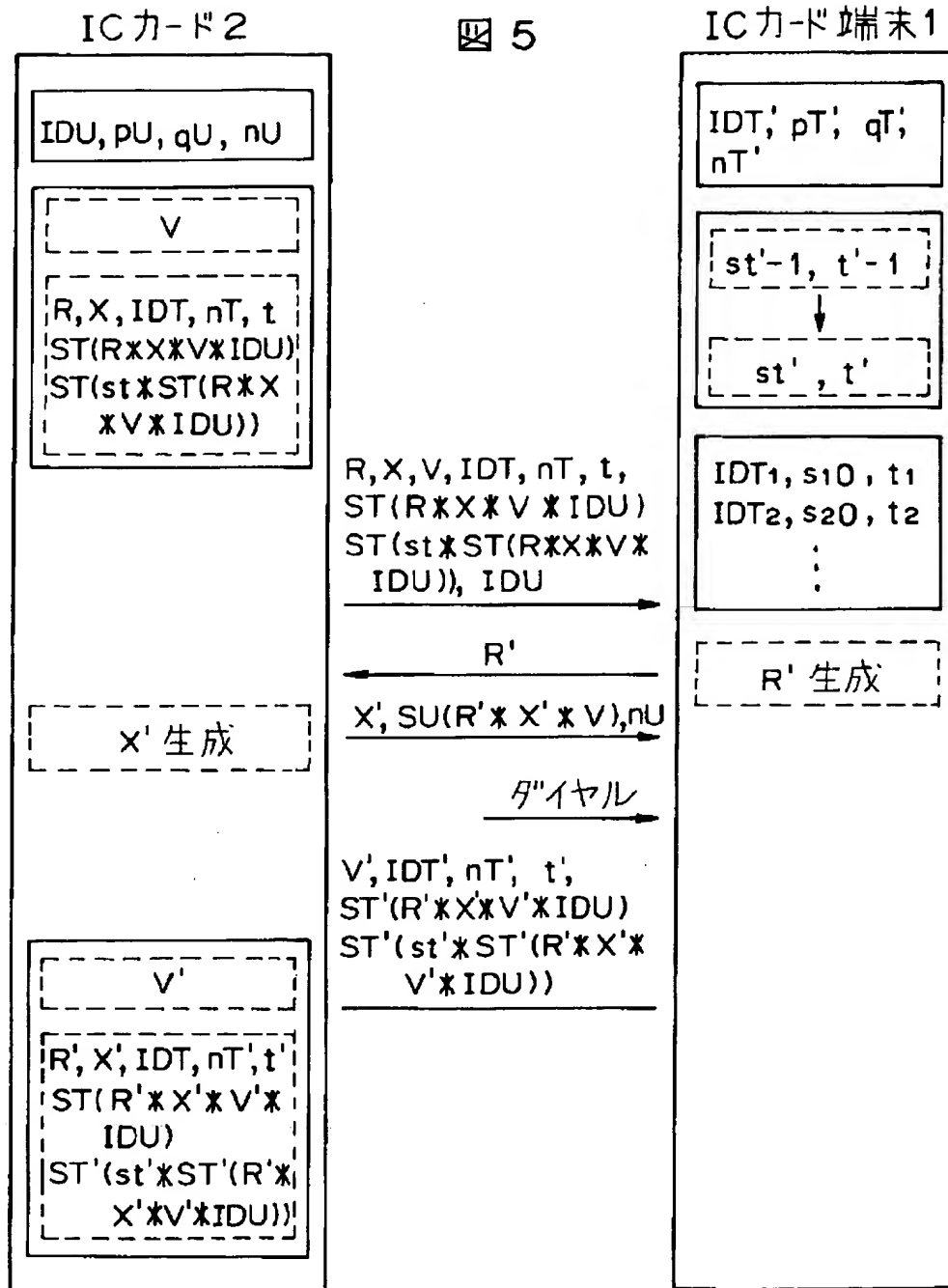


【図4】

図 4



【図5】



フロントページの続き

(72)発明者 宮口 庄司
 東京都千代田区内幸町1丁目1番6号 日
 本電信電話株式会社内

(72)発明者 岡本 龍明
 東京都千代田区内幸町1丁目1番6号 日
 本電信電話株式会社内

(72)発明者 藤岡 淳
東京都千代田区内幸町1丁目1番6号 日
本電信電話株式会社内